Remarks/Arguments

Initially, Applicant thanks the Examiner for considering the reference listed in the Information Disclosure Statement dated January 28, 2003.

Applicant has amended claim 19 to correct a typographical error in the preamble. Claim 19, as amended, now recites "A monitoring system as recited in claim 11, ..."

The Examiner has objected to the Declaration asserting that it is defective because it does not state that the Declarant reviewed and understood the contents of the specification, including the claims. Applicant respectfully disagrees. The Declaration and Power of Attorney submitted on October 29, 2001 (copy attached) specifically states, at page 1, "I have reviewed and understand the contents of the above-identified specification, including the claims." This Declaration is signed by the sole inventor, Matthew Campagna, on page 2. As such, Applicant respectfully requests that the Examiner withdraw the objection to the Declaration.

Claims 1-20 are pending in this application. Claims 1, 11, and 20 are independent claims. Claims 1-8 stand rejected under 35 U.S.C. § 102(e) as being anticipated by Ranger et al. (U.S. Patent No. 6,393,568). Further, claims 9-20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Ranger, in view of Birrell et al. (U.S. Patent No. 5,805,803). Applicant respectfully traverses these rejections based on the following remarks.

The present invention addresses a basic problem associated with Secure Socket Layer (SSL) protocol communications received or transmitted from a network resource (client 1) which resides behind a firewall. Given the secure nature of SSL, the firewall does not have access to the encrypted communications. (Spec. at 0002) Accordingly, the use of SSL prevents the firewall (TCM server 3) from reading and filtering the encrypted communications in the application layer data. (Spec. at 0002).

The present invention solves this problem by requiring the client 1 to securely transmit to the TCM server 3 the Pre-Master-Secret and the negotiated ciphersuite previously established between the client 1 and the Internet SSL server 5. (Spec. at 0016). The SSL communications between client 1 and Internet SSL server 5 are then permitted with the TCM server 3 intercepting and decrypting the same in its capacity as a firewall and a virus detector.

Given this background, claim 1 of the present invention recites, among other things, exchanging information between a client and a target server to create and decode cryptographically protected data, and sending, to a monitoring server, enabling data associated with the exchanged information, which allows the monitoring server to decode the cryptographically protected data. Simply put, the "enabling data" (the Pre-Master-Secret and negotiated ciphersuite) allows the monitoring server (TCM server 3) to decode the "cryptographically protected data" (the SSL communications) between the client 1 and the Internet SSL server 5. It is respectfully submitted that neither of the cited references disclose, teach or suggest these limitations, either alone or in combination.

The Examiner asserts that Ranger "teaches" exchanging information, although the Examiner does not indicate which parties are exchanging information or the type of information being exchanged. It is irrelevant whether or not Ranger teaches anything. Instead, the proper starting point under § 102(e) is whether or not Ranger "discloses" the recited exchanging information between the client and the target server? Ranger does not.

As noted above with respect to claim 1, a client and a target server exchange SSL information such as the Pre-Master-Secret and the negotiated ciphersuite. This information enables both the client and the target server to create and decode cryptographically protected data during the SSL communications. While Ranger addresses obtaining decoding information (a data header includes decryption information, col. 7, lines 11-14), there is no disclosure of a client and a target server exchanging such information.

Further, in claim 1, the recited enabling data is associated with the information exchanged between the client and the target server (the Pre-Master-Secret and negotiated ciphersuite are associated with the SSL communications). Accordingly, even though Ranger addresses decryption information (col. 7, lines 11-14, for example), there is no disclosure that such decryption information is related, in any way, to any information exchanged between a client and a target server. In fact, since Ranger fails to disclose any exchange of information between a client and a target server, Ranger cannot disclose the recited sending of the associated enabling data. As such, Ranger fails to anticipate at least two (2) recited limitations of independent claims 1.

With respect to the § 103(a) rejection of independent claims 11 and 20, the Examiner admits that Ranger fails to teach the use of a Secure Socket Layer (SSL) in a private

network. Instead, the Examiner asserts that Birrell supplies this missing limitation. Applicant respectfully disagrees.

Initially, it must be pointed out that the communications between Birrell's client 110 and the specified resource 160 are not secure along the entire length of the channel, as recited in claims 11 and 20 (claim 11, establish an SSL communication channel, claim 20, cryptographically protected data transmitted between client and target server). In particular, client 110 communicated securely with proxy server 143 (HTTPS = HTTP and SSL). (Col. 4, lines 13-17). On the other hand, specified resource 160 communicates with proxy server 143 in a non-secure manner (non-secure HTTP protocol). (Col. 4, lines 52-64).

As such, from the specified resource 160 to the client 110, at least one portion of the communications channel remains non-secure. Specifically, the communications channel between the specified resource 160 and the proxy server 143 is always non-secure. Therefore, the Examiner's asserted combination would not produce the present invention, as claimed in claims 11 and 20.

It is irrelevant whether or not Birrell teaches or suggests establishing a secure tunnel, as asserted by the Examiner. A secure tunnel does not change the nature of the non-secure channel between the proxy server 143 and the specifies resource 160. Since Birrell cannot supply all of the elements missing from Ranger, claims 11 and 20 are not obvious in view of the Examiner's asserted combination of Ranger and Birrell. For at least the same reasons as set out above with respect to independent claims 1 and 11, dependant claims 2-10 and 12-19 are also allowable over the Examiner's applied art.

Further, independent claims 11 and 20, also recite corresponding limitations to those set out above with respect to claim 1 (exchanging information between a client and a target server and sending enabling data associated with the information exchanged). Ranger fails to disclose these limitations. On the other hand, Birrell fails to disclose, teach, or suggest these two (2) missing limitations, and the Examiner has not argued otherwise.

It is not enough that Birrell allegedly teaches, suggests, or discloses an SSL in a private network, as asserted by the Examiner. As noted above, the relevant claims recite, among other things, exchanging information between a client and a target server to create and decode cryptographically protected data and to establish an SSL communication session (claim 9) and to establish an SSL communication channel through which cryptographically

protected data is exchanged (claim 11). Birrell fails to address establishing a complete SSL channel between a client and an outside internet server.

In support of the asserted combination, the Examiner claims that one of ordinary skill would utilize the SSL firewall connection disclosed in Birrell because transferred data could include a virus harmful to the system. However, as noted above, Birrell's communication channel is not an SSL channel throughout its entire length. Moreover, the Examiner has failed to cite any portion of either reference, either alone or in combination, for the required motivation to combine. Similarly, neither reference, either alone or in combination, supplies the required motivation to combine, and the Examiner has not argued otherwise. As such, the Examiner's § 103(a) rejection of claims 9-20, based on the asserted combination of Ranger and Birrell, is improper. These claims must, therefore, be allowed.

In view of the foregoing amendments and remarks, it is respectfully submitted that the claims of this application are now in a condition for allowance and favorable action thereon is requested.

Respectfully submitted,

Eric P. Halber
Reg. No. 46,378
Attorney of Record
Telephone (203) 924-3852

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000